CLAIMS

1. A system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems, the communication means including a transport entity for providing transport services, and a transport-independent, session-level security entity logically positioned above the transport entity and visible to the local application entity, the security entity being operative to set up secure communication sessions with peer security entities in other systems and comprising:

- key-exchange handshake means for conducting a handshake with a said peer security entity associated with a particular remote application entity with which said local application entity wishes to communicate, this handshake involving the exchange of key-related data for use in generating session keys; and
- secure channel means for enabling messages to be passed between the local application entity and said particular remote application entity with authentication and/or encryption of these messages being effected using the session keys generated from said key-related data whereby to secure these messages in passage between the cooperating security entities;

the handshake means being operative when conducting said handshake to exchange attribute justifications, in the form of one or more certificates, with said peer security entity to enable verification by each system that the application entity being contacted has the particular attributes, if any, required by its own application entity.

2. A system according to claim 1, wherein the security entity is capable of establishing multiple concurrent security sessions with another system over a common transport connection set up by the transport entity.

3. A system according to claim 1, wherein the handshake means is operative to indicate to said remote application during the course of handshake services and attributes required of said remote application by the local application entity, the handshake means being further operative to receive back an indication of attributes that the remote application requires of the local application.

4. A system according to claim 1, further comprising attribute justification means for proving from certificates received form the remote system during said handshake that the remote application has the required attributes.

5. A system according to claim 1, wherein said local application entity is a mediation entity acting on behalf of one or more other application entities.

6. A system according to claim 1, wherein said handshake is a three message handshake in the course of which:

- an authenticated ephemeral Diffie-Hellman key exchange is effected
- a cipher suite is negotiated determining the authentication and/or encryption algorithms that will be subsequently used by the secure channel means for the security session concerned;
- advisories regarding the attributes required by the local and remote applications of each other are exchanged; and
- justifications for the required attributes are exchanged.

7. A system according to claim 1, wherein the security entity formats its communications intended for the remote peer security entity in protocol data units (PDUs) that each include:

- a session indicator enabling the peer security entity to determine to which security session the PDU relates; and
- a message-type field by which the peer security entity can determine whether the PDU carries handshake-related data or a message being passed over the secure channel of the security session indicated by said session indicator.